КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

А.К. Гуц

Доклад в Сибирском автотранспортном колледже

12 мая 2021 года

Содержание

Содержание

Содержание

Содержание

КК сегодня

Руководитель проектного офиса по квантовым технологиям госкорпорации "Росатом"и глава недавно созданной в России Национальной квантовой лаборатории Руслан Юнусов:

> *В России есть программа, на которую выделено 24 миллиарда рублей. Через три года мы должны создать 100-кубитный прототип квантового компьютера, а также разработать софт и алгоритмы. Задача, конечно, грандиозная. Но выполнимая. Как создать 100-кубитный прототип квантового компьютера к 2024 году – мы понимаем. А вот как выйти в лидеры в этой области – пока нет.*

КК сегодня

Китай сейчас собирается потратить на очередной квантовый центр 11 миллиардов долларов.

IBM предоставила всем онлайн свой 53-кубитовый КК IBM Quantum Experience.

МГУ объявил о создании аналогичной облачной платформы под свой КК.

Как видим, ведущие страны стремятся создать квантовый компьютер, на котором будут вестись квантовые вычисления.

Так что такое квантовый компьютер и квантовые вычисления?

КК IBM

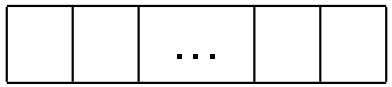
Архитектура КК

Квантовый компьютер имеет архитектуру, аналогичную классическому компьютеру. Он состоит из:

– регистров памяти,
– процессора, построенного из логических элементов и производящего вычисления,
– устройства ввода информации,
– устройства вывода полученной в ходе вычислений информации.

Регистры

Память компьютера разбита на регистры. Регистры состоят из некоторого количества разрядов. Регистр из m разрядов изобразим как



(квадратик изображает разряд)

Классический разряд $\square$ хранит единицу информации – *бит* информации – 0 или 1.

Запишем разряд в символическом виде

$$|n_k\rangle, \quad n_k = 0, 1.$$

Тогда классический регистр можно представить как

$$|n_{m-1} n_{m-2} \ldots n_0\rangle. \tag{1}$$

Для технической реализации бита используются разные

Классический регистр

Состояние классического регистра в момент времени t

Разряд классического регистра находится только в одном из двух возможных состояний – $|0\rangle$ или $|1\rangle$. Поэтому состояние регистра – это

$$|n_{m-1}n_{m-2}\ldots n_0\rangle.$$

Например, состояние

$$|\underbrace{01001011100011\ldots}_{m}\rangle$$

Кубит и квантовый регистр

Квантовый разряд $\square$ хранит единицу информации – квантовый бит, или *кубит*, информации – 0 или 1.

Кубит и квантовый регистр

Квантовый разряд $\square$ хранит единицу информации – квантовый бит, или *кубит*, информации – 0 или 1.

Квантовый разряд в символическом виде выглядит так же, как классический:

$$|n_k\rangle, \quad n_k = 0, 1.$$

И поэтому квантовый регистр представляется в виде

$$|n_{m-1} n_{m-2} \ldots n_0\rangle. \tag{2}$$

Кубит и квантовый регистр

Квантовый разряд $\square$ хранит единицу информации – квантовый бит, или *кубит*, информации – 0 или 1.

Квантовый разряд в символическом виде выглядит так же, как классический:

$$|n_k\rangle, \quad n_k = 0, 1.$$

И поэтому квантовый регистр представляется в виде

$$|n_{m-1} n_{m-2} \ldots n_0\rangle. \tag{2}$$

Для технической реализации кубита предлагаются разные физические устройства, основой которых является любая двухуровневая (квантовомеханическая) система (спин, фотон, атом, молекула, ион).

Квантовое состояние

Состояние квантового регистра в момент времени t

Разряд квантового регистра находится в состоянии

$$\alpha|0\rangle + \beta|1\rangle, \qquad \alpha, \beta \in C.$$

Поэтому состояние квантового m-разрядного регистра – это *когерентная суперпозиция* всех *базисных состояний*:

$$|\psi(t)\rangle \equiv \sum_{n_{m-1}=0}^{1} \sum_{n_{m-2}=0}^{1} \dots \sum_{n_0=0}^{1} c_{n_{m-1}n_{m-2}\dots n_0} |n_{m-1}n_{m-2}\dots n_0\rangle,$$

$$c_{n_{m-1}n_{m-2}\dots n_0} \in C.$$

Числа $|c_{n_{m-1}n_{m-2}\dots n_0}|^2$ интерпретируются как вероятность пребывания регистра в состоянии $|n_{m-1}n_{m-2}\dots n_0\rangle$.

Квантовое состояние

Например, возможно следующее состояние КК

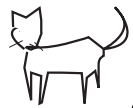
$$|\psi(t)\rangle \equiv c_1|\underbrace{01001011100011...}_{m}\rangle +$$

$$+ c_2|\underbrace{11001011100011...}_{m}\rangle + ...$$

Иначе говоря, КК в момент t находится сразу во всех возможных классических состояниях классического регистра.

Квантовое состояние

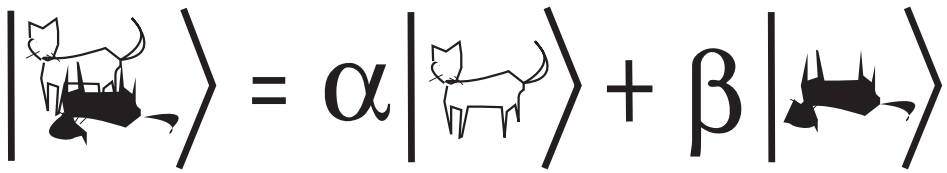
Комментарий. Состояние 1-разрядного регистра квантового компьютера в момент времени t подобно одновременному пребыванию кота в живом и мёртвом состоянии:

$$\left|\text{  }\right\rangle = \alpha\left|\text{  }\right\rangle + \beta\left|\text{  }\right\rangle$$

Иначе говоря, в квантовом мире альтернативы могут существовать одновременно.

Квантовое состояние

Комментарий. Состояние 1-разрядного регистра квантового компьютера в момент времени t подобно одновременному пребыванию кота в живом и мёртвом состоянии:



Иначе говоря, в квантовом мире альтернативы могут существовать одновременно.

Впрочем, можно предположить, что квантовый компьютер находится сразу во множестве параллельных вселенных. В случае кота – в одной вселенной кот жив, а в другой – мёртв. Наблюдатель видит только того кота, в какой вселенной живет сам; параллельный, другой мир он не видит. Такой подход называется эвереттовской интерпретацией квантовой механики.

Классический процессор

Процессор классического компьютера состоит из схем, собранных из логических элементов.

Логические элементы – это технические устройства, реализующие некоторые логические операции классической логики.

Процессор преобразует, меняет содержание разрядов регистра посредством каждого, входящего в него логического элемента U:

$$U : |n_{m-1}n_{m-2}...n_0\rangle \rightarrow |n'_{m-1}n'_{m-2}...n'_0\rangle. \qquad (3)$$

Квантовый процессор

Квантовый процессор также состоит из логических элементов, называемых *гейтами*.

В теории квантового компьютера существует бесконечное количество логических элементов. Однако доказано, что квантовый компьютер может быть построен всего из двух логических элементов: однокубитового $\widehat{Q}(\theta, \varphi)$ и 2-кубитового «$\widehat{CNOT}$» (управляемое НЕ).

Квантовый процессор

Квантовый процессор преобразует, меняет содержание разрядов квантового регистра посредством каждого входящего в него логического элемента (гейта) $\widehat{U}$:

$$\widehat{U}: \sum_{n_{m-1}=0}^{1} \sum_{n_{m-2}=0}^{1} \dots \sum_{n_0=0}^{1} c_{n_{m-1}n_{m-2}\dots n_0} |n_{m-1}n_{m-2}\dots n_0\rangle \rightarrow$$

$$\rightarrow \sum_{n_{m-1}=0}^{1} \sum_{n_{m-2}=0}^{1} \dots \sum_{n_0=0}^{1} c_{n_{m-1}n_{m-2}\dots n_0} |n'_{m-1}n'_{m-2}\dots n'_0\rangle. \quad (4)$$

Как видно из формулы (4), **в один шаг изменены сразу все 2^m значений базисных состояний**. Это *эффект параллелизма* в работе квантового компьютера, не имеющий места для классических компьютеров. Для такой производительности за один шаг потребовалось бы 2^m классических процессоров. Если $m = 16$, то $2^{16} = 65536$!

Квантовая сцепленность (запутанность)

Состояние

$$\sum_{n_{m-1}=0}^{1} \sum_{n_{m-2}=0}^{1} \dots \sum_{n_0=0}^{1} c_{n_{m-1}n_{m-2}\dots n_0} |n_{m-1}n_{m-2}\dots n_0\rangle \qquad (5)$$

квантового регистра называется *сцепленным*, если оно **не может** быть представлено в виде

$$|x_1\rangle \dots |x_m\rangle, \qquad (6)$$

где $|x_j\rangle = \alpha_j|0\rangle + \beta_j|1\rangle$ $(j = 1, \dots, m)$.
Если состояние регистра (5) не является сцепленным, то это означает фактическое наличие в распоряжении для вычислений классического регистра вида (6). Отсутствуют другие, параллельные базовые состояния и, следовательно, отсутствует эффект квантового параллелизма, существенно ускоряющего работу компьютера.

Пример сцепленности

Запишем сцепленное состояние объекта «брак» формулами. Надо всего лишь учесть альтернативу в случае гибели мужа:

$$\text{Брак} = |\textbf{жив}\rangle_{\text{м}}|\textbf{замужняя}\rangle_{\text{ж}} + |\textbf{мёртв}\rangle_{\text{м}}|\textbf{вдова}\rangle_{\text{ж}},$$

где буквы «м» и «ж» метят состояния мужчины и женщины соответственно.

Вычисление

КК – это физическое устройство, содержащее достаточно большое число $N > 100$ кубитов.
Подготовка к по вычислению состоит из шагов:

- Входной регистр приводится в исходное основное базисное состояние
$$|\underbrace{00...0}_{m}\rangle.$$
- Обеспечиваются большое время декогеренции (не менее чем 104 раза больше времени выполнения основных квантовых операций (время такта)).
Декогеренция – это взаимодействие системы кубитов с окружающей средой. Она приводит к разрушению суперпозиций квантовых состояний и делает невозможным выполнение квантовых алгоритмов.

- Обеспечивается возможность измерения состояния квантовой системы на выходе, т. е. при выводе результата.
- Обеспечивается сцепленность начальных данных, представляющих квантовую суперпозици.

Ввод начальных данных

С помощью последовательного применения к состоянию $|\underbrace{00...0}_{m}\rangle$ гейтов

$$\hat{U}^{(1)}, \hat{U}^{(2)}, ..., \hat{U}^{(m)}, \hat{U}^{(k)} = \hat{I} \otimes ... \otimes \hat{I} \otimes \underbrace{\hat{U}_1}_{k} \otimes \hat{I} \otimes ... \otimes \hat{I},$$

где $\hat{U}^{(k)}$ действует только на k-й кубит посредством гейта $\hat{U}_1$, преобразующего однокубитовое состояние, квантовый регистр приводится в m-кубитовое состояние, являющееся *когерентной суперпозицией* всех базисных состояний:

$$\hat{U}^{(m)}\hat{U}^{(m-1)}...\hat{U}^{(1)} : |\underbrace{00...0}_{m}\rangle \rightarrow \hat{U}^{(m)}\hat{U}^{(m-1)}...\hat{U}^{(1)}|\underbrace{00...0}_{m}\rangle =$$

$$\equiv \sum_{n_{m-1}=0}^{1} \sum_{n_{m-2}=0}^{1} ... \sum_{n_0=0}^{1} c_{n_{m-1}n_{m-2}...n_0}|n_{m-1}n_{m-2}...n_0\rangle, \quad \sum_{n=0}^{2^m-1} |c_n|^2 = 1$$

Вычисление

Вычисление – это преобразование $\widehat{U}_F$ начального состояния:

$$\widehat{U}_F\left(\sum_{n=0}^{2^m-1} c_n|n\rangle\right) = \sum_{n=0}^{2^m-1} c_n \widehat{U}_F|n\rangle = \sum_{n=0}^{2^m-1} c_n|F(n)\rangle, \qquad (7)$$

$$|n\rangle = |n_{m-1}\ldots n_0\rangle,$$

$$n = (n_{m-1}\ldots n_0)_2 = \sum_{k=1}^{m} n_{m-k}2^{m-k} \rightleftarrows |n_{m-1}\ldots n_0\rangle.$$

Конкретная реализация преобразования $\widehat{U}_F$ представляет собой запрограммированный квантовый алгоритм вычисления значений функции F.

Вывод результата

Вывод результата в квантовом компьютеринге – это *измерение* квантового состояния (7):

$$\sum_{n=0}^{2^m-1} c_n |F(n)\rangle \to |F(n)\rangle.$$

В силу принципа квантовой механики вмешательство измеряющего устройства (устройство вывода данных) означает декогеренцию, т.е. разрушение когерентного состояния (7). Мы получаем значение $F(n)$ лишь с вероятностью $|c_n|^2$.

Получаемый на выходе результат вычислений вследствие декогеренции, как видим, носит *вероятностный характер*! Иначе говоря, то, что получено на выходе – состояние (регистра) $|F(n)\rangle$, верно лишь с некоторой вероятностью $|c_n|^2$.

Спасибо за внимание!